VIRTUAL PRIVATE LINE NETWORK CONNECTION CONTROL METHOD, VIRTUAL PRIVATE LINE NETWORK CONNECTION CONTROLLER AND VIRUTAL PRIVATE LINE NETWORK CONNECTION SYSTEM

Publication number: JP2002077261

Publication date: 2002-03-15

Inventor: MATSUMOTO MASAAKI; IBUKI MOTOSHI; OKUMURA SATOSHI; SATO KATSUHIKO

Applicant: NIPPON TELEGRAPH & TELEPHONE

Classification:

- international: ***H04M3/42; H04L12/56; H04M11/00;*** **H04M3/42; H04L12/56; H04M11/00;** (IPC1-7): H04L12/56; H04M3/42; H04M11/00

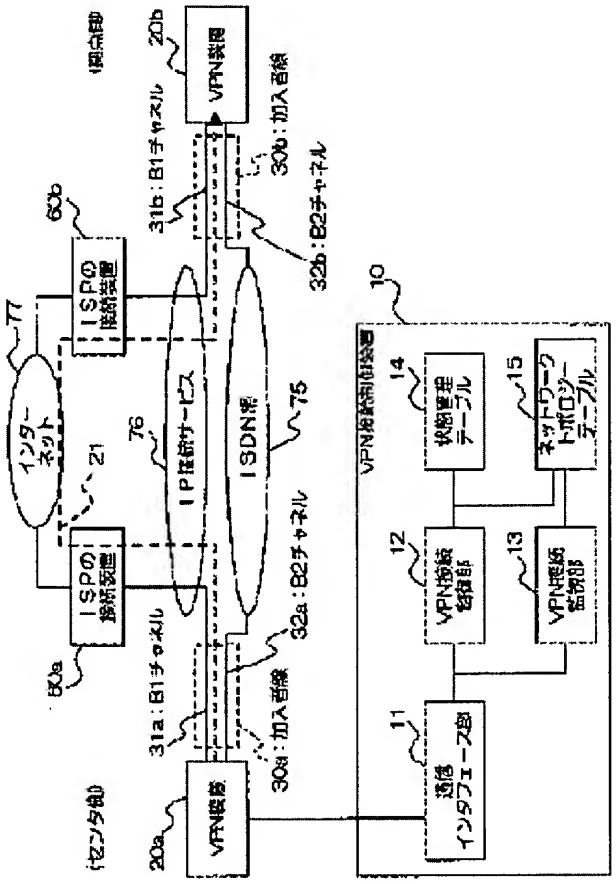
- european:

Application number: JP20000264551 20000831

Priority number(s): JP20000264551 20000831

Abstract of **JP2002077261**

PROBLEM TO BE SOLVED: To provide a virtual private line network connection control method, its controller and system for connecting VPN devices which even in a communication environment where an IP address is dynamically allocated such as internet connection by means of dial-up. SOLUTION: The instruction of connection to the Internet is given to the VPN device 20b of a stronghold-side from a VPN connection control part 12, installed in a VPN connection controller 10 via the VPN device 20a and a B2 channel 32a on a center-side and an ISDN network 75. The VPN device 20b receives the instruction and connects it to the connection device 60b of ISP, by using a B1 channel 31b and receives the allocation of the IP address from ISP. The IP address is notified to the VPN connection control part 12 and is written into a state managing table 14. Then, the IP address of the VPN device of a calling destination side is transmitted to the VPN device of a calling source side by communication by using the B2 channel.



(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号
特開2002－77261
（P2002－77261A）
(43)公開日　平成14年３月15日(2002.3.15)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード（参考）
Ｈ０４Ｌ　12/56		Ｈ０４Ｍ　3/42	Ａ	５Ｋ０２４
Ｈ０４Ｍ　3/42		11/00	３０２	５Ｋ０３０
11/00	３０２	Ｈ０４Ｌ　11/20	１０２Ａ	５Ｋ１０１

審査請求　未請求　請求項の数10　ＯＬ　（全 11 頁）

(21)出願番号　特願2000－264551(P2000－264551)

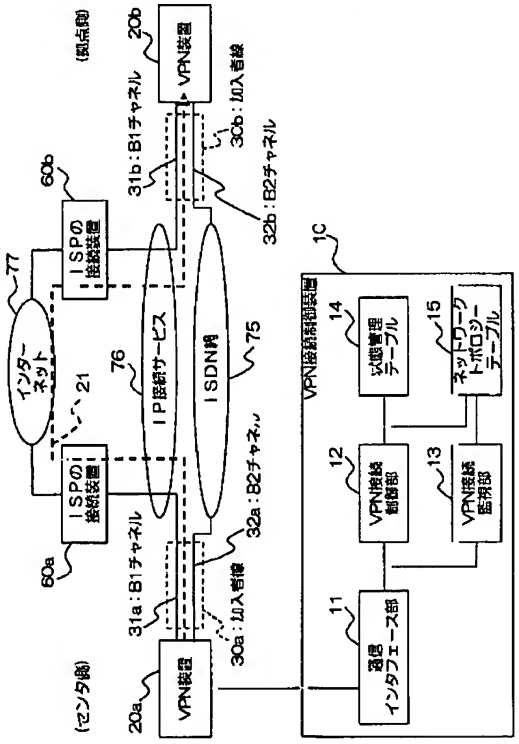
(22)出願日　平成12年８月31日(2000.8.31)

(71)出願人　399041158
西日本電信電話株式会社
大阪府大阪市中央区馬場町３番15号
(72)発明者　松本　政昭
大阪府大阪市中央区馬場町３番15号　西日本電信電話株式会社内
(72)発明者　伊吹　元志
大阪府大阪市中央区馬場町３番15号　西日本電信電話株式会社内
(74)代理人　100064908
弁理士　志賀　正武

最終頁に続く

(54)【発明の名称】　仮想専用線網接続制御方法および仮想専用線網接続制御装置ならびに仮想専用線網接続システム

(57)【要約】
【課題】　ダイヤルアップによるインターネット接続など、ＩＰアドレスが動的に割り振られる通信環境においても、ＶＰＮ装置同士の接続を可能とする仮想専用線網接続制御方法およびその装置、システムを提供する。
【解決手段】　ＶＰＮ接続制御装置１０に設けられたＶＰＮ接続制御部１２からセンタ側のＶＰＮ装置２０ａおよびＢ２チャネル３２ａ、ＩＳＤＮ網７５を経由して拠点側のＶＰＮ装置２０ｂにインターネットへの接続を指示する。この指示を受けて、ＶＰＮ装置２０ｂはＢ１チャネル３１ｂを用いてＩＳＰの接続装置６０ｂに接続するとともに、ＩＳＰからＩＰアドレスの割り当てを受ける。このＩＰアドレスは、ＶＰＮ接続制御部１２に通知され、状態管理テーブル１４に書き込まれる。それとともに、Ｂ２チャネルを用いた通信によって、発呼先側のＶＰＮ装置のＩＰアドレスが発呼元側のＶＰＮ装置に伝えられる。



【特許請求の範囲】
【請求項１】　複数の仮想専用線網装置によって構成される仮想専用線網接続システムの接続を制御する仮想専用線網接続制御装置であって、
前記仮想専用線網装置に動的に割り振られる通信アドレスを保持する管理テーブルと、
各々の前記仮想専用線網装置に動的に割り振られた通信アドレスを受け取って前記管理テーブルに書き込み、発呼先の前記仮想専用線網装置の通信アドレスを前記管理テーブルから読み出して発呼元の前記仮想専用線網装置に通知することによって接続を制御する仮想専用線網接続制御部と、
を備えることを特徴とする仮想専用線網接続制御装置。
【請求項２】　前記仮想専用線網装置は、電話加入者線上の複数の通信チャネルを使用した通信を行い、そのうちの第１の通信チャネルをパブリックなデータ通信網に接続することによってアプリケーションデータを伝送するために使用し、他の第２の通信チャネルを前記通信アドレスの通知を含む接続制御のために使用するものであり、
前記管理テーブルは、前記仮想専用線網装置の前記第２の通信チャネルを用いた通信のための電話番号を保持するものであり、
前記仮想専用線網接続制御部は、前記第１の通信チャネルを前記パブリックなデータ通信網に接続する旨の指示を発呼先の前記仮想専用線網装置に通知するために当該発呼先の前記仮想専用線網装置の前記電話番号を前記管理テーブルから読み出してセンタ側の前記仮想専用線網装置に渡し、センタ側の前記仮想専用線網装置から当該発呼先の前記仮想専用線網装置に動的に割り振られた通信アドレスを受け取って前記管理テーブルに書き込み、発呼元の前記仮想専用線網装置に発呼先の前記仮想専用線網装置の通信アドレスを通知するために前記管理テーブルから発呼先の前記仮想専用線網装置の通信アドレスと発呼元の前記仮想専用線網装置の前記電話番号とを読み出してセンタ側の前記仮想専用線網装置に渡すことによって接続を制御することを特徴とする請求項１に記載の仮想専用線網接続制御装置。
【請求項３】　接続が確立された前記仮想専用線網装置の接続状態を監視する仮想専用線網接続監視部を備え、
前記仮想専用線網接続制御部は、前記仮想専用線網接続監視部によって切断が検知された仮想専用線網装置がある場合には、この切断された仮想専用線網装置に関して再度接続を制御する手順を実行することを特徴とする請求項１または２に記載の仮想専用線網接続制御装置。
【請求項４】　仮想専用線網接続における呼の発呼元および発呼先の前記仮想専用線網装置の関係を保持するネットワークトポロジーテーブルを備え、
前記仮想専用線網接続制御部は、前記ネットワークトポロジーテーブルのデータに含まれる発呼先の前記仮想専用線網装置のみに関して接続を制御する手順を実行することを特徴とする請求項１から３までのいずれかに記載の仮想専用線網接続制御装置。
【請求項５】　パブリックなデータ通信網における相手側の通信アドレスを指定することによってアプリケーションデータを相互に伝送しあう複数の仮想専用線網装置によって構成される仮想専用線網接続システムであって、
電話加入者線の第１の通信チャネルを用いて前記パブリックなデータ通信網に接続し、このパブリックなデータ通信網上で仮想専用線網の呼を設定し前記アプリケーションデータを伝送するとともに、電話加入者線の第２の通信チャネルを用いて前記通信アドレスの通知を含む接続制御のための通信を行う複数の仮想専用線網装置と、
前記仮想専用線網装置に動的に割り振られる前記パブリックなデータ通信網の通信アドレスと前記仮想専用線網装置の前記第２の通信チャネルを用いた通信のための電話番号を保持する管理テーブルを備え、前記第１の通信チャネルを用いて前記パブリックなデータ通信網に接続する旨の指示を発呼先の前記仮想専用線網装置に通知するために当該発呼先の前記仮想専用線網装置の前記電話番号を前記管理テーブルから読み出してセンタ側の前記仮想専用線網装置に渡し、センタ側の前記仮想専用線網装置から当該発呼先の前記仮想専用線網装置に動的に割り振られた前記通信アドレスを受け取って前記管理テーブルに書き込み、発呼元の前記仮想専用線網装置に発呼先の前記仮想専用線網装置の通信アドレスを通知するために前記管理テーブルから発呼先の前記仮想専用線網装置の通信アドレスと発呼元の前記仮想専用線網装置の前記電話番号とを読み出してセンタ側の前記仮想専用線網装置に渡すことによって接続を制御する仮想専用線網接続制御装置と、
によって構成され、
センタ側の前記仮想専用線網装置は前記第１の通信チャネルを用いて前記パブリックなデータ通信網に接続する旨の指示を、前記仮想専用線網接続制御装置から発呼先の前記仮想専用線網装置に通知するために発呼先の前記仮想専用線網装置の前記電話番号を受け取った際には前記第２の通信チャネルを用いて当該電話番号に対する通信を設定してこの指示を通知し、当該発呼先の前記仮想専用線網装置に動的に割り振られた通信アドレスをこの仮想専用線網装置から受け取った際にはこの通信アドレスを前記仮想専用線網接続制御装置に渡し、前記仮想専用線網接続制御装置から発呼元の前記仮想専用線網装置に発呼先の前記仮想専用線網装置の通信アドレスを通知するために前記管理テーブルから発呼先の前記仮想専用線網装置の通信アドレスと発呼元の前記仮想専用線網装置の前記電話番号とを受け取った際には前記第２の通信チャネルを用いて当該電話番号に対する通信を設定して当該発呼先の前記仮想専用線網装置の通信アドレスを通

知することを特徴とする仮想専用線網接続システム。
【請求項６】　前記仮想専用線網接続制御装置は、接続が確立された前記仮想専用線網装置の接続状態を監視し、接続が切断された前記仮想専用線網装置を検知した場合には、この切断された仮想専用線網装置に関して再度接続を制御する手順を実行することを特徴とする請求項５に記載の仮想専用線網接続システム。
【請求項７】　前記仮想専用線網接続制御装置は、仮想専用線網接続における呼の発呼元および発呼先の前記仮想専用線網装置の関係を保持するネットワークトポロジーテーブルを備え、前記ネットワークトポロジーテーブルのデータに含まれる発呼先の前記仮想専用線網装置のみに関して接続を制御する手順を実行することを特徴とする請求項５または６に記載の仮想専用線網接続システム。
【請求項８】　第１の通信チャネルおよび第２の通信チャネルを使用可能でありパブリックなデータ通信網上で相手側の通信アドレスを指定することによってアプリケーションデータを相互に伝送しあう複数の仮想専用線網装置と、これらの仮想専用線網装置間の接続を制御する仮想専用線網接続制御装置とによって構成される仮想専用線網接続システムにおける仮想専用線網接続制御方法であって、
仮想専用線網接続制御装置が自己の保有する管理テーブルから発呼先の前記仮想専用線網装置の電話番号を読み出して該電話番号をセンタ側の前記仮想専用線網装置に渡し、この電話番号を受け取ったセンタ側の前記仮想専用線網装置が前記第２の通信チャネルを使用してこの電話番号に対する通信を設定する第１の過程と、
センタ側の前記仮想専用線網装置が、前記第２の通信チャネルを通して、発呼先の前記仮想専用線網装置に対して、前記パブリックなデータ通信網に接続する旨の指示を行う第２の過程と、
この指示を受けた発呼側の前記仮想専用線網装置が、前記第１の通信チャネルを用いて前記パブリックなデータ通信網に接続する第３の過程と、
当該発呼側の仮想専用線網装置に動的に割り振られた前記パブリックなデータ通信網における通信アドレスを、当該発呼側の仮想専用線網装置からセンタ側の前記仮想専用線網装置を経由して前記仮想専用線網接続制御装置に通知し、これを受けた前記仮想専用線網接続制御装置が前記管理テーブルにこの通信アドレスを書き込む第４の過程と、
前記仮想専用線網接続制御装置が前記管理テーブルから発呼元の前記仮想専用線網装置の電話番号と発呼先の前記仮想専用線網装置の前記通信アドレスとを読み出してセンタ側の前記仮想専用線網装置に渡し、これを受けたセンタ側の前記仮想専用線網装置が前記第２の通信チャネルを用いて当該電話番号に対する呼を設定して当該発呼元の仮想専用線網装置に対して当該発呼先の仮想専用線網装置の通信アドレスを通知する第５の過程と、
この通知を受けた発呼元の前記仮想専用線網装置が当該通信アドレスを用いて前記パブリックなデータ通信網上で発呼先の前記仮想専用線網装置との間の呼を設定する第６の過程と、
を有することを特徴とする仮想専用線網接続制御方法。
【請求項９】　前記仮想専用線網接続制御装置が、接続が確立された前記仮想専用線網装置の接続状態を監視する接続監視過程と、
前記接続監視過程において切断が検知された仮想専用線網装置がある場合には、前記仮想専用線網接続制御装置がこの切断された仮想専用線網装置に関して再度接続を制御する再接続過程と、を有することを特徴とする請求項８に記載の仮想専用線網接続制御方法。
【請求項１０】　仮想専用線網接続における呼の発呼元および発呼先の前記仮想専用線網装置の関係を保持するネットワークトポロジーテーブルのデータに含まれる発呼先の前記仮想専用線網装置のみに関して前記第１から第６までの過程の手順を実行することを特徴とする請求項８または９に記載の仮想専用線網接続制御方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】この発明は、主としてインターネットを用いて、仮想的な専用線網を構築するための複数の仮想専用線網装置間の接続を制御する仮想専用線網接続制御装置およびその方法に関する。
【０００２】
【従来の技術】従来の技術において、仮想専用線網（以下では、ＶＰＮ（Virtual Private Network ）と略称する）は以下のように構築されていた。複数の拠点にそれぞれＶＰＮ装置を設置し、各ＶＰＮ装置の通信アドレスを予め管理情報として保持しておく。また、各々のＶＰＮ装置は近くのアクセスポイントを通してインターネットに接続可能としておく。そして、予め定義されたネットワークトポロジー情報に従って、発呼元のＶＰＮ装置が発呼先の通信アドレスを指定してインターネット経由での接続を確立することにより、このＶＰＮを介した通信が可能となる。なお、上記のＶＰＮ装置間の通信はＩＰ（インターネットプロトコル）によって行われ、通信アドレスとしてはＩＰアドレスが用いられる。
【０００３】
【発明が解決しようとする課題】公衆網を利用してＩＳＰ（インターネットサービスプロバイダ）に対してダイヤルアップ接続を行うような通信環境においては、予め固定的なＩＰアドレスが割り振られているのではなく、ダイヤルアップ接続時に、例えばＤＨＣＰ（Dynamic Host Configuration Protocol ）などを用いて動的にＩＰアドレスが割り振られるようになっていることが多い。このような動的なアドレス割当ては、限りあるＩＰアドレス（グローバルＩＰアドレス）の空間を有効に活用す

ること、および、ＩＳＰ側のアドレス管理のための手間とコストを軽減することなどを目的としている。

【０００４】しかしながら、上記従来技術では、各ＶＰＮ装置のＩＰアドレスを予め保持しておくことが前提となっているため、固定的なＩＰアドレスをＶＰＮ装置に割当てることのできる通信環境でしかＶＰＮを構築できないという問題があった。そこで、ＩＰアドレスが予め固定されてないダイヤルアップ接続などの通信環境においても、利用可能なＶＰＮ装置が求められている。

【０００５】本発明は、上記のような事情を考慮してなされて物であり、ダイヤルアップによるインターネット接続など、ＩＰアドレスが動的に割り振られる通信環境においても、ＶＰＮ装置同士の接続を可能とする仮想専用線網接続制御方法および仮想専用線網接続制御装置ならびに仮想専用線網接続システムを提供することを目的とする。

【０００６】

【課題を解決するための手段】上記の課題を解決するために、この発明による仮想専用線網接続制御装置は、複数の仮想専用線網装置によって構成される仮想専用線網接続システムの接続を制御する仮想専用線網接続制御装置であって、前記仮想専用線網装置に動的に割り振られる通信アドレスを保持する管理テーブルと、各々の前記仮想専用線網装置に動的に割り振られた通信アドレスを受け取って前記管理テーブルに書き込み、発呼先の前記仮想専用線網装置の通信アドレスを前記管理テーブルから読み出して発呼元の前記仮想専用線網装置に通知することによって接続を制御する仮想専用線網接続制御部とを備えることを特徴とする。

【０００７】また、この発明による仮想専用線網接続制御装置においては、前記仮想専用線網装置は、電話加入者線上の複数の通信チャネルを使用した通信を行い、そのうちの第１の通信チャネルをパブリックなデータ通信網に接続することによってアプリケーションデータを伝送するために使用し、他の第２の通信チャネルを前記通信アドレスの通知を含む接続制御のために使用するものであり、前記管理テーブルは、前記仮想専用線網装置の前記第２の通信チャネルを用いた通信のための電話番号を保持するものであり、前記仮想専用線網接続制御部は、前記第１の通信チャネルを前記パブリックなデータ通信網に接続する旨の指示を発呼先の前記仮想専用線網装置に通知するために当該発呼先の前記仮想専用線網装置の前記電話番号を前記管理テーブルから読み出してセンタ側の前記仮想専用線網装置に渡し、センタ側の前記仮想専用線網装置から当該発呼先の前記仮想専用線網装置に動的に割り振られた通信アドレスを受け取って前記管理テーブルに書き込み、発呼元の前記仮想専用線網装置に発呼先の前記仮想専用線網装置の通信アドレスを通知するために前記管理テーブルから発呼先の前記仮想専用線網装置の通信アドレスと発呼元の前記仮想専用線網装置の前記電話番号とを読み出してセンタ側の前記仮想専用線網装置に渡すことによって接続を制御することを特徴とする。ここで、電話加入者線上の複数の通信チャネルとは、例えばＩＳＤＮ（Integrated Services Digital Networks，統合デジタルサービス網）における複数のチャネルである。例えば、加入者線毎に２本のＢチャネルと１本のＤチャネルが収容される「２Ｂ＋Ｄ」の構成である場合、２本のうちの１本のＢチャネルを前記第１の通信チャネルとして使用し、他の１本のＢチャネルを前記第２の通信チャネルとして使用することができる。また、使用可能な通信チャネルの数がより多い場合、例えば２３本のＢチャネルと１本のＤチャネルとで構成される「２３Ｂ＋Ｄ」の構成の場合には、第１の通信チャネルとして複数のＢチャネルを割当てても良いし、第２の通信チャネルとして複数のＢチャネルを割当てても良い。また、ここで、パブリックなデータ通信網の代表例はインターネットである。このようなパブリックなデータ通信網は比較的低コストで利用できるため、これを用いて仮想的な専用線網を構築する場合、実際に専用回線をリースする場合に比べて安価な実現が可能となる。

【０００８】また、この発明による仮想専用線網接続制御装置においては、接続が確立された前記仮想専用線網装置の接続状態を監視する仮想専用線網接続監視部を備え、前記仮想専用線網接続制御部は、前記仮想専用線網接続監視部によって切断が検知された仮想専用線網装置がある場合には、この切断された仮想専用線網装置に関して再度接続を制御する手順を実行することを特徴とする。

【０００９】また、この発明による仮想専用線網接続制御装置においては、仮想専用線網接続における呼の発呼元および発呼先の前記仮想専用線網装置の関係を保持するネットワークトポロジーテーブルを備え、前記仮想専用線網接続制御部は、前記ネットワークトポロジーテーブルのデータに含まれる発呼先の前記仮想専用線網装置のみに関して接続を制御する手順を実行することを特徴とする。

【００１０】また、この発明による仮想専用線網接続システムは、パブリックなデータ通信網における相手側の通信アドレスを指定することによってアプリケーションデータを相互に伝送しあう複数の仮想専用線網装置によって構成される仮想専用線網接続システムであって、電話加入者線の第１の通信チャネルを用いて前記パブリックなデータ通信網に接続し、このパブリックなデータ通信網上で仮想専用線網の呼を設定し前記アプリケーションデータを伝送するとともに、電話加入者線の第２の通信チャネルを用いて前記通信アドレスの通知を含む接続制御のための通信を行う複数の仮想専用線網装置と、前記仮想専用線網装置に動的に割り振られる前記パブリックなデータ通信網の通信アドレスと前記仮想専用線網装

置の前記第２の通信チャネルを用いた通信のための電話番号を保持する管理テーブルを備え、前記第１の通信チャネルを用いて前記パブリックなデータ通信網に接続する旨の指示を発呼先の前記仮想専用線網装置に通知するために当該発呼先の前記仮想専用線網装置の前記電話番号を前記管理テーブルから読み出してセンタ側の前記仮想専用線網装置に渡し、センタ側の前記仮想専用線網装置から当該発呼先の前記仮想専用線網装置に動的に割り振られた前記通信アドレスを受け取って前記管理テーブルに書き込み、発呼元の前記仮想専用線網装置に発呼先の前記仮想専用線網装置の通信アドレスを通知するために前記管理テーブルから発呼先の前記仮想専用線網装置の通信アドレスと発呼元の前記仮想専用線網装置の前記電話番号とを読み出してセンタ側の前記仮想専用線網装置に渡すことによって接続を制御する仮想専用線網接続制御装置とによって構成され、センタ側の前記仮想専用線網装置は前記第１の通信チャネルを用いて前記パブリックなデータ通信網に接続する旨の指示を、前記仮想専用線網接続制御装置から発呼先の前記仮想専用線網装置に通知するために発呼先の前記仮想専用線網装置の前記電話番号を受け取った際には前記第２の通信チャネルを用いて当該電話番号に対する通信を設定してこの指示を通知し、当該発呼先の前記仮想専用線網装置に動的に割り振られた通信アドレスをこの仮想専用線網装置から受け取った際にはこの通信アドレスを前記仮想専用線網接続制御装置に渡し、前記仮想専用線網接続制御装置から発呼元の前記仮想専用線網装置に発呼先の前記仮想専用線網装置の通信アドレスを通知するために前記管理テーブルから発呼先の前記仮想専用線網装置の通信アドレスと発呼元の前記仮想専用線網装置の前記電話番号とを受け取った際には前記第２の通信チャネルを用いて当該電話番号に対する通信を設定して当該発呼先の前記仮想専用線網装置の通信アドレスを通知することを特徴とする。

【００１１】また、この発明による仮想専用線網接続システムにおいては、前記仮想専用線網接続制御装置は、接続が確立された前記仮想専用線網装置の接続状態を監視し、接続が切断された前記仮想専用線網装置を検知した場合には、この切断された仮想専用線網装置に関して再度接続を制御する手順を実行することを特徴とする。

【００１２】また、この発明による仮想専用線網接続システムにおいては、前記仮想専用線網接続制御装置は、仮想専用線網接続における呼の発呼元および発呼先の前記仮想専用線網装置の関係を保持するネットワークトポロジーテーブルを備え、前記ネットワークトポロジーテーブルのデータに含まれる発呼先の前記仮想専用線網装置のみに関して接続を制御する手順を実行することを特徴とする。

【００１３】また、この発明による仮想専用線網接続制御方法は、第１の通信チャネルおよび第２の通信チャネルを使用可能でありパブリックなデータ通信網上で相手側の通信アドレスを指定することによってアプリケーションデータを相互に伝送しあう複数の仮想専用線網装置と、これらの仮想専用線網装置間の接続を制御する仮想専用線網接続制御装置とによって構成される仮想専用線網接続システムにおける仮想専用線網接続制御方法であって、仮想専用線網接続制御装置が自己の保有する管理テーブルから発呼先の前記仮想専用線網装置の電話番号を読み出して該電話番号をセンタ側の前記仮想専用線網装置に渡し、この電話番号を受け取ったセンタ側の前記仮想専用線網装置が前記第２の通信チャネルを使用してこの電話番号に対する通信を設定する第１の過程と、センタ側の前記仮想専用線網装置が、前記第２の通信チャネルを通して、発呼先の前記仮想専用線網装置に対して、前記パブリックなデータ通信網に接続する旨の指示を行う第２の過程と、この指示を受けた発呼側の前記仮想専用線網装置が、前記第１の通信チャネルを用いて前記パブリックなデータ通信網に接続する第３の過程と、当該発呼側の仮想専用線網装置に動的に割り振られた前記パブリックなデータ通信網における通信アドレスを、当該発呼側の仮想専用線網装置からセンタ側の前記仮想専用線網装置を経由して前記仮想専用線網接続制御装置に通知し、これを受けた前記仮想専用線網接続制御装置が前記管理テーブルにこの通信アドレスを書き込む第４の過程と、前記仮想専用線網接続制御装置が前記管理テーブルから発呼元の前記仮想専用線網装置の電話番号と発呼先の前記仮想専用線網装置の前記通信アドレスとを読み出してセンタ側の前記仮想専用線網装置に渡し、これを受けたセンタ側の前記仮想専用線網装置が前記第２の通信チャネルを用いて当該電話番号に対する呼を設定して当該発呼元の仮想専用線網装置に対して当該発呼先の仮想専用線網装置の通信アドレスを通知する第５の過程と、この通知を受けた発呼元の前記仮想専用線網装置が当該通信アドレスを用いて前記パブリックなデータ通信網上で発呼先の前記仮想専用線網装置との間の呼を設定する第６の過程とを有することを特徴とする。

【００１４】また、この発明による仮想専用線網接続制御方法においては、前記仮想専用線網接続制御装置が接続が確立された前記仮想専用線網装置の接続状態を監視する接続監視過程と、前記接続監視過程において切断が検知された仮想専用線網装置がある場合には前記仮想専用線網接続制御装置がこの切断された仮想専用線網装置に関して再度接続を制御する再接続過程とを有することを特徴とする。

【００１５】また、この発明による仮想専用線網接続制御方法は、仮想専用線網接続における呼の発呼元および発呼先の前記仮想専用線網装置の関係を保持するネットワークトポロジーテーブルのデータに含まれる発呼先の前記仮想専用線網装置のみに関して前記第１から第６までの過程の手順を実行することを特徴とする。

【００１６】
【発明の実施の形態】以下、図面を参照しこの発明の一実施形態について説明する。本実施形態では、ＩＰアドレスが固定されていないダイヤルアップ接続環境でＶＰＮ接続するため、複数のＶＰＮ装置のうちの１台をセンタ側ＶＰＮ装置と位置付け、そのセンタ側ＶＰＮ装置に、各ＶＰＮ装置の電話番号、ＩＰアドレス、接続／切断のフラグを管理するテーブルを備えたＶＰＮ接続制御装置を併設することとする。例えば、ＶＰＮ接続を構築する企業においては、センタ側ＶＰＮ装置を本店に設置し、その他の拠点側ＶＰＮ装置を支店や営業所等に設置する。
【００１７】この構成によりＶＰＮ接続する場合の手順は、次の通りである。（１）ＩＳＤＮ回線のＢ２チャネルを利用して、センタ側ＶＰＮ装置から拠点側ＶＰＮ装置に対して接続要求を行う。（２）これを受けた拠点側ＶＰＮ装置は、ダイヤルアップによってＩＳＰの接続装置に対して接続要求を行い、ＩＳＰの接続装置から通知されたＩＰアドレスを、センタ側ＶＰＮ装置を介してＶＰＮ接続制御装置に通知する。（３）ＶＰＮ接続制御装置は、各拠点側ＶＰＮ装置から通知されたＩＰアドレスをテーブルに記録する。（４）ＶＰＮ接続制御装置は、各ＶＰＮ装置に対し、それぞれのＶＰＮ装置の接続先となるＶＰＮ装置のＩＰアドレスを送信し、これを受信したＶＰＮ装置はＶＰＮ接続制御装置からそのＩＰアドレスに対する接続を行い、ＶＰＮ接続を確立する。（５）接続完了後、ＶＰＮ接続制御装置は各ＶＰＮ装置の接続状態を監視し、何らかの原因で接続が切断された場合には、そのＶＰＮ装置に対し前記（１）から（４）に示した接続手順を実行し、接続の再構築を行う。
【００１８】図１は、本実施形態によるＶＰＮ接続システム（仮想専用線網接続システム）の構成を示す構成図である。図１において、符号２０ａおよび２０ｂはそれぞれセンタ側および拠点側のＶＰＮ装置（仮想専用線網装置）、３０ａおよび３０ｂはそれぞれＶＰＮ装置２０ａおよび２０ｂに接続されたＩＳＤＮの加入者線である。加入者線３０ａには、時分割多重化方式により複数のチャネルが論理的に収容されており、その中にはＢ１チャネル３１ａ（第１の通信チャネル）およびＢ２チャネル３２ａ（第２の通信チャネル）が含まれている。また、加入者線３０ｂには同様にＢ１チャネル３１ｂおよびＢ２チャネル３２ｂが含まれている。また、７５はＩＳＤＮ網、７６は加入者線を利用してＩＳＰ等への接続を行うためのＩＰ接続サービス、７７はインターネット（パブリックなデータ通信網）である。また、６０ａおよび６０ｂは、それぞれセンタ側および拠点側から接続するためのＩＳＰの接続装置である。
【００１９】図１に示す構成においては、センタ側のＶＰＮ装置２０ａはＢ１チャネル３１ａを使用してＩＳＰの接続装置６０ａに接続でき、拠点側のＶＰＮ装置２０ｂはＢ１チャネル３１ｂを使用してＩＳＰの接続装置６０ｂに接続できるようになっている。これにより、インターネット７７を経由する経路２１によって、ＶＰＮ装置２０ａと２０ｂとの間での通信が可能となる。また、それぞれのＶＰＮ接続装置は、Ｂ２チャネル３２ａおよび３２ｂを用いてＩＳＤＮ網７５を経由して相互に通信を行うことが可能である。
【００２０】また、１０は、センタ側ＶＰＮ装置２０ａに接続されておりＶＰＮ装置間の接続を制御するためのＶＰＮ接続制御装置（仮想専用線網接続制御装置）であり、このＶＰＮ接続制御装置１０は、内部に通信インタフェース部１１とＶＰＮ接続制御部１２とＶＰＮ接続監視部１３と状態管理テーブル１４（管理テーブル）とネットワークトポロジーテーブル１５とを有している。
【００２１】図２は、状態管理テーブル１４のデータ構造およびデータ例を示す表図である。図２に示すように、状態管理テーブル１４は、ＶＰＮ装置名、ＩＳＤＮ番号、グローバルＩＰアドレス、状態をデータ項目として持つ表形式のデータである。これらのデータ項目のうち、グローバルＩＰアドレスは、各ＶＰＮ装置に割り振られたＩＰアドレスがＶＰＮ接続制御装置に通知されたときに書き込まれる。また、状態は、各ＶＰＮ装置から接続／切断が通知されたときやＶＰＮ接続監視部１３によって状態変化が検出されたときに書き換えられる。図２に示すデータ例では、Ａ～Ｅの５つのＶＰＮ装置を管理する情報が状態管理テーブルによって保持されている。なお、本例では、Ａがセンタ側のＶＰＮ装置であり、Ｂ～Ｅの４つが拠点側のＶＰＮ装置である。
【００２２】次に、ＶＰＮ接続制御装置１０の制御によって、各ＶＰＮ装置が自己以外のすべてのＶＰＮ装置に対して接続を行うための手順を説明する。図５は、その手順を示すフローチャートである。
【００２３】（ステップＳ１１）図５の手順において、まず、ＶＰＮ接続制御装置１０のＶＰＮ接続制御部１２が状態管理テーブル１４を参照する。そして、ＶＰＮ制御装置１０からセンタ側（サーバ側）のＶＰＮ装置に対する指示により、センタ側のＶＰＮ装置Ａは、状態が「接続」ではないすべてのＶＰＮ装置に対して（図２に示すデータ例においては、ＶＰＮ装置ＤおよびＥに対して）、Ｂ２チャネルを用いてＩＳＤＮ網経由での呼設定を行う。なお、その際には状態管理テーブル１４から得られるＩＳＤＮ番号が用いられる。
（ステップＳ１２）そして、センタ側のＶＰＮ装置Ａは、接続先のＶＰＮ装置に対して、ＩＰ接続サービスへのダイヤルアップを行うように依頼する。
【００２４】（ステップＳ１３）上記の依頼を受けた拠点側のＶＰＮ装置は、Ｂ１チャネルを用いたダイヤルアップによってＩＳＰの接続装置に接続する。
（ステップＳ１４）そして、拠点側のＶＰＮ装置は、接続したＩＳＰの接続装置から自己のグローバルＩＰアド

レスを取得する。このグローバルＩＰアドレスは、拠点側のＶＰＮ装置からＢ２チャネルを用いてセンタ側のＶＰＮ装置に通知され、さらにＶＰＮ接続制御装置１０のＶＰＮ接続制御制御部に伝えられて状態管理テーブル１４に書き込まれる。なお、センタ側のＶＰＮ装置自体の状態が「接続」でない場合にも、上記と同様に、Ｂ１チャネルを用いてＩＳＰの接続装置への接続が行われ、割り振られたグローバルＩＰアドレスが状態管理テーブル１４に書き込まれる。

【００２５】（ステップＳ１５）すべてのＶＰＮ装置がインターネットに接続されると、Ｂ２チャネルを用いた通信により、状態管理テーブルに管理されている全ＶＰＮ装置のグローバルＩＰアドレスが各々のＶＰＮ装置に通知される。

（ステップＳ１６）上記の通知を受けた各ＶＰＮ装置は、通知を受けたＩＰアドレスに対してＶＰＮトンネルを設定する。

【００２６】（ステップＳ１７）ＶＰＮ接続監視部１３は、所定の時間間隔ですべてのＶＰＮ装置に対して監視信号を送出し、接続状態を監視する。そして、その状況に応じて適宜、状態管理テーブル１４の状態の項目を更新する。ここで、もしいずれかのＶＰＮ接続装置から監視信号に対する応答がなく切断と判断した場合には、ステップＳ１１に戻って再接続の手順を実行する。また、監視信号に対して正常応答が得られた場合には、正常接続状態にあると認識するとともに、次の監視信号送出のタイミングまで待つ。正常接続状態においては、ステップＳ１６において設定されたＶＰＮトンネルを通して、ＶＰＮのアプリケーションデータがＶＰＮ装置間で伝送される。

【００２７】図６は、上記接続手順によって、全ＶＰＮ装置間で相互に接続が設定されたときのネットワークトポロジーを示す参考図である。図６において、Ａ～Ｅはそれぞれ ＶＰＮ監視装置を表わし、それらを結ぶ矢印線はＶＰＮ装置間の接続を表わす。なお、矢印線の根元側が発呼元であり、先側が発呼先である。

【００２８】上に述べた方法では、例えば営業所－営業所間のように通信トラフィックが無いもしくは非常に少ない対地においてもＶＰＮトンネルを構築し、監視信号を全てのＶＰＮ装置に送るため、ネットワーク上に不必要に多くのパケットを送出することになるとともに、営業所等のＶＰＮ装置にも高い負荷をかけることとなってしまう。そこで、例えば、本社－支店間、本社－営業所間、支店－営業所間など通信の必要がある対地間のみにＶＰＮトンネルを設定する方法を次に説明する。

【００２９】図３は、ネットワークトポロジーを定義するためのネットワークトポロジーテーブル１５のデータ構造及びデータ例を示す表図である。このネットワークトポロジーテーブルは、発呼元ＶＰＮ装置名と発呼先ＶＰＮ装置名の項目を有しており、各ＶＰＮ装置をノードとする有向グラフと等価なデータを表形式で保持している。その有向グラフのノードがＶＰＮ装置間で確立される接続を表わしている。図３に示すデータ例は、Ａ（発呼元）→Ｂ（発呼先）、Ｂ→Ａ、Ｃ→Ａ、Ｃ→Ｂ、Ｄ→Ａ、Ｄ→Ｂ、Ｅ→Ａ、Ｅ→Ｂの接続によってＶＰＮを構築することを表わしている。

【００３０】図７は、ネットワークトポロジーテーブルを参照しながら、必要な対地間のみで接続を行うための手順を示すフローチャートである。

【００３１】（ステップＳ２１）図７の手順において、まず、ＶＰＮ接続制御装置１０のＶＰＮ接続制御部１２がネットワークトポロジーテーブル１５を参照する。そして、発呼先ＶＰＮ装置名となっているＶＰＮ装置のＩＳＤＮ番号を状態管理テーブル１４から取得する。そして、センタ側（サーバ側）のＶＰＮ装置からこれら発呼先のＶＰＮ装置に対して、Ｂ２チャネルを用いてダイヤルし、ＩＳＤＮ網の呼を設定する。例えば、図３に示したデータ例の場合、発呼先ＶＰＮ装置名の項目に含まれているのは「Ａ」および「Ｂ」の２つであり、これらのＶＰＮ装置のＩＳＤＮ番号は図２に示したデータ例によると、それぞれ「０６－４８０３－１１１１」および「０６－４８０４－２２２２」である。なお、ここで、ＡからＢへはＢ２チャネルを用いたダイヤルは行われるが、Ａはセンタ側ＶＰＮ装置そのものであるので、ＡからＡへのダイヤルは行う必要はない。

【００３２】（ステップＳ２２）次に、センタ側のＶＰＮ装置から各発呼先のＶＰＮ装置に対して、ＩＰ接続サービスへのダイヤルアップを行うように指示が行われる。

（ステップＳ２３）この指示に基づき、各発呼先ＶＰＮ装置は、Ｂ１チャネルを用いて、ＩＳＰの接続装置への接続を行う。なお、図３に示すようにセンタ側ＶＰＮ装置（Ａ）が発呼先ＶＰＮ装置に含まれている場合には、センタ側ＶＰＮ装置からもＩＳＰ接続装置への接続が行われる。

（ステップＳ２４）そして、ＩＳＰの接続装置への接続を行ったＶＰＮ装置は、ＩＳＰからグローバルＩＰアドレスを取得し、そのグローバルＩＰアドレスはセンタ側のＶＰＮ装置を経由してＶＰＮ接続制御部１２に伝えられ、ＶＰＮ接続制御部１２によって状態管理テーブル１４に書き込まれる。

【００３３】（ステップＳ２５）次に、ＶＰＮ接続制御部１２は、ネットワークトポロジーテーブル１５を参照し、発呼元となっているそれぞれのＶＰＮ装置に関して、その発呼元ＶＰＮ装置のＩＳＤＮ番号を状態管理テーブル１４から取得するとともに、各発呼元ＶＰＮ装置に対応する発呼先ＶＰＮ装置のグローバルＩＰアドレスを同じく状態管理テーブル１４から取得する。そして、センタ側ＶＰＮ装置は、Ｂ２チャネルを用いて各々の発呼元ＶＰＮ装置のＩＳＤＮ番号をダイヤルし、その発呼

元ＶＰＮ装置に対して、対応する発呼先ＶＰＮ装置のグローバルＩＰアドレスを通知する。例えば、図2および図3に示すデータ例の場合、ネットワークトポロジーテーブル１５には発呼元ＶＰＮ装置名として「Ｂ」が含まれており、この「Ｂ」に対応する発呼先ＶＰＮ装置名は「Ａ」となっている。従って、センタ側ＶＰＮ装置は、状態管理テーブル１４に書かれているＢのＩＳＤＮ番号「０６－４８０４－２２２２」をダイヤルしてＶＰＮ装置Ｂに接続し、Ａのグローバルアドレス「ｘ．ｘ．ｘ．ｘ」を通知する。また、例えば、ネットワークトポロジーテーブル１５に発呼元ＶＰＮ装置名として含まれている「Ｄ」に関して、この「Ｄ」に対応する発呼先ＶＰＮ装置名は「Ａ」および「Ｂ」であるので、センタ側ＶＰＮ装置は、ＶＰＮ装置ＤのＩＳＤＮ番号「０６－４８０６－４４４４」をダイヤルしてＶＰＮ装置Ｄに接続し、ＶＰＮ装置ＡおよびＢのグローバルＩＰアドレス「ｘ．ｘ．ｘ．ｘ」および「ｙ．ｙ．ｙ．ｙ」を通知する。なお、ここではＩＰアドレスを「ｘ．ｘ．ｘ．ｘ」および「ｙ．ｙ．ｙ．ｙ」と表わしたが、実際には具体的な数値によって構成されるアドレスが通知される。

【００３４】（ステップＳ２６）そして、通知を受けた各々の発呼元ＶＰＮ装置は、必要に応じてＩＳＰの接続装置に接続してから、通知されたＩＰアドレスに対してＶＰＮトンネルを設定する。

（ステップＳ２７）ＶＰＮ接続監視部１３は、所定の時間間隔ですべての発呼先となっているＶＰＮ装置に対して監視信号を送出し、設定状態を監視する。そして、その状況に応じて適宜、状態管理テーブル１４の状態の項目を更新する。ここで、もしいずれかのＶＰＮ接続装置から監視信号に対する応答がなく切断と判断した場合には、ステップＳ２１に戻って再接続の手順を実行する。また、監視信号に対して正常応答が得られた場合には、正常接続状態にあると認識するとともに、次の監視信号送出のタイミングまで待つ。

【００３５】この手順によると、ネットワークトポロジーテーブルに従って、限られたＶＰＮ装置間のみにＶＰＮトンネルを設定し、発呼先となっているＶＰＮ装置のみに監視信号を送出するため、ネットワーク上に不必要に多くのパケットを送出することもなく、営業所等のＶＰＮ装置の負荷を軽減することが可能となる。また、これにより、営業所等のＶＰＮ装置の性能規模を小さくすることもできるため、システム全体のコストを抑制することが可能となる。

【００３６】図8は、上記接続手順によって、ネットワークトポロジーテーブルに定義されたＶＰＮ装置間のみで接続が設定されたときのネットワークトポロジーを示す参考図である。図8に示すように、ＶＰＮ装置Ａからはのみに、同じくＢからはＡのみに、またＣ，Ｄ，Ｅからはそれぞれ ＡおよびＢのみに対して発呼が行われている。

【００３７】次に、予め定められたタイムスケジュールに従ってＶＰＮ接続の設定をさらに限定する方法について説明する。なおこの方法は、ネットワークトポロジーテーブルに定義された全ての接続に関して２４時間３６５日フルに呼を設定する必要がない場合に有用である。図4は、ＶＰＮ装置毎の稼動スケジュールを情報として含む状態管理テーブルのデータ構造およびデータ例を示す表図である。この図に示す状態管理テーブルには、ＶＰＮ装置名とＩＳＤＮ番号とグローバルＩＰアドレスと状態のほかに、スケジュールがデータ項目として付加された表形式のデータである。図４に示すデータ例では、ＶＰＮ装置Ａは停止することなくフル稼働するスケジュールとなっており、ＶＰＮ装置Ｂは土曜日および日曜日に停止、ＶＰＮ装置Ｃ～Ｅは平日の日勤帯のみ稼動するというスケジュールになっている。そして、ＶＰＮ接続制御部１２は、ＶＰＮ接続制御装置１０に内蔵されているカレンダー機能および時計機能の情報を参照することによって、この状態管理テーブルに定義されたスケジュールに従って、稼動させるべきＶＰＮ装置接続させるような制御を行う。つまり、各ＶＰＮ装置が稼動すべき時間帯においてのみ、そのＶＰＮ装置に関する初期起動や接続監視を行う。また、稼動すべき時間帯の終了時点には、ＶＰＮ接続を切断する手順を行う。

【００３８】上述したＶＰＮ接続制御装置は、例えば、コンピュータシステムを用いて実現する。具体的には、ＶＰＮ接続制御部１２およびＶＰＮ接続監視部１３は、図5や図7を用いて説明した手順に応じた処理をプログラムの形式でコンピュータシステムの記憶装置に記憶しておき、中央処理装置がそのプログラムを読み出して実行することによって実現する。また、通信インタフェース部１１は、コンピュータシステムの入出力装置およびそれを駆動するプログラムによって実現し、ケーブル等を介してＶＰＮ装置２０ａと信号のやりとりを行うとともに、その信号内容に応じた情報をＶＰＮ接続制御部１２やＶＰＮ接続監視部１３との間で授受する。そして、状態管理テーブル１４およびネットワークトポロジーテーブル１５は、その構造に応じた表現形式のデータをコンピュータシステムの記憶装置に記憶させることによって実現する。ここで、記憶装置とは、例えば、磁気ディスクや半導体メモリなどを用いる。

【００３９】

【発明の効果】以上説明したように、この発明によれば、仮想専用線網接続制御装置に仮想専用線網装置に動的に割り振られる通信アドレスを保持する管理テーブルを備え、発呼先仮想専用線網装置の通信アドレスを仮想専用線網接続制御装置から発呼元仮想専用線網装置に通知するため、発呼元側に予め固定的な通信アドレスの情報を設定しておかなくても、発呼元側から発呼先側に呼を設定し、仮想専用線網の接続を実現することができる。従って、例えばＩＰ接続サービスのダイヤルアップ

接続のように通信アドレスが動的に割り振られるような通信環境においても、固定的な通信アドレスが割り振られる常時接続サービスと同等の接続を実現できる。具体的には、例えば、ダイヤルアップによるインターネット接続を利用した仮想専用線網の構築が可能となる。

【００４０】また、この発明によれば、接続が確立された後、例えば監視用のパケットを用いるなどして仮想専用線網装置の接続状態を監視し、接続が切断された場合には再接続の手順を実行するため、障害時にも自動的な接続の復旧を試みる耐障害性の高い仮想専用線網を実現することが可能となる。

【００４１】また、この発明によれば、仮想専用線網接続制御装置に接続の方向性を考慮したネットワークトポロジーテーブルを備え、このネットワークトポロジーテーブルに仮想専用線網装置の発呼元および発呼先の関係を定義し、この情報に基づいて呼の設定を行うとともに、このテーブルに発呼先と定義された仮想専用線網装置のみについて上記の接続監視を行うため、監視信号を必要最低限に抑え、仮想専用線網装置の負荷を軽減し、不要なパケットトラヒックの排除を行うことによって、より一層実効効率の高いデータ転送を行う仮想専用線網を実現することが可能となる。

【図面の簡単な説明】

【図１】　この発明の一実施形態によるＶＰＮ接続システムの構成を示す構成図である。

【図２】　同実施形態によるＶＰＮ接続制御装置に設けられた状態管理テーブル（１４）のデータ構造およびデータの一例を示す表図である。

【図３】　同実施形態によるＶＰＮ接続制御装置に設けられたネットワークトポロジーテーブル（１５）のデータ構造およびデータの一例を示す表図である。

【図４】　同実施形態によるＶＰＮ接続制御装置に設けられた状態管理テーブル（１４）のデータ構造およびデータの他の例を示す表図である。

【図５】　同実施形態によるＶＰＮ接続制御の手順を示すフローチャートである。

【図６】　同実施形態により、全ＶＰＮ装置間で相互に接続が設定されたときのネットワークトポロジーを示す参考図である。

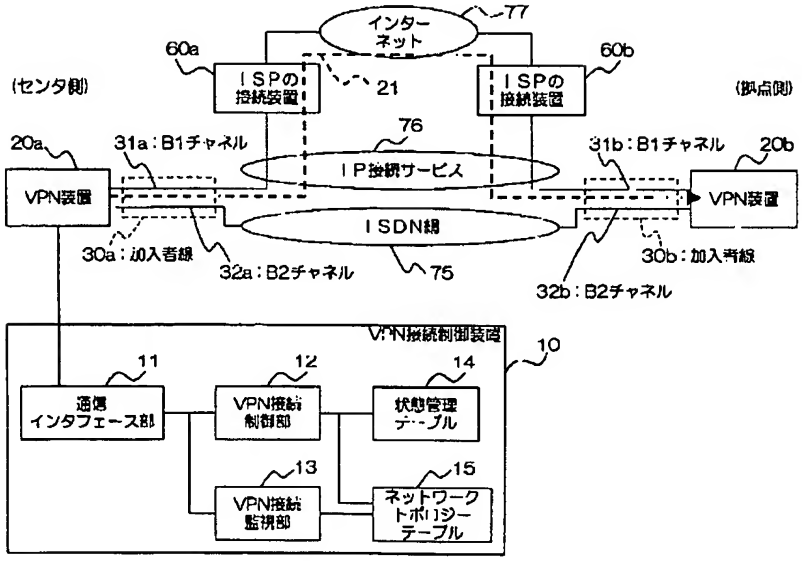
【図７】　同実施形態により、ネットワークトポロジーテーブルを参照しながら、必要な対地間のみで接続を行う手順を示すフローチャートである。

【図８】　同実施形態により、ネットワークトポロジーテーブルに定義されたＶＰＮ装置間のみで接続が設定されたときのネットワークトポロジーの一例を示す参考図である。

【符号の説明】

１０　ＶＰＮ接続制御装置
１１　通信インタフェース部
１２　ＶＰＮ接続制御部
１３　ＶＰＮ接続監視部
１４　状態管理テーブル
１５　ネットワークトポロジーテーブル
２０ａ，２０ｂ　ＶＰＮ装置
３０ａ，３０ｂ　加入者線
３１ａ，３１ｂ　Ｂ１チャネル
３２ａ，３２ｂ　Ｂ２チャネル
６０ａ，６０ｂ　ＩＳＰの接続装置
７５　ＩＳＤＮ網
７６　ＩＰ接続サービス
７７　インターネット

【図１】



【図３】

発呼元VPN装置名	発呼先VPN装置名
A	B
B	A
C	A,B
D	A,B
E	A,B

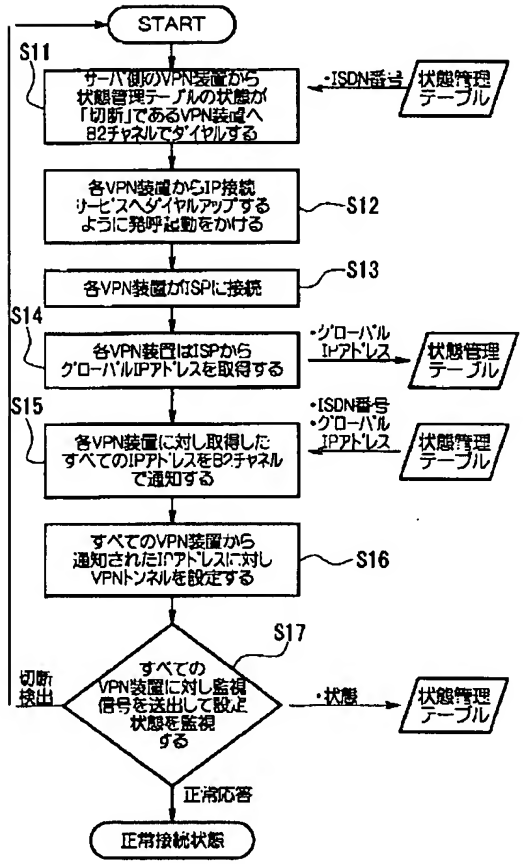
【図2】

VPN装置名	ISDN番号	グローバルIPアドレス	状態
A	06-4803-1111	X.X.X.X	接続
B	06-4804-2222	Y.Y.Y.Y	接続
C	06-4805-3333	Z.Z.Z.Z	接続
D	06-4806-4444	V.V.V.V	切断
E	06-4807-5555	W.W.W.W	切断

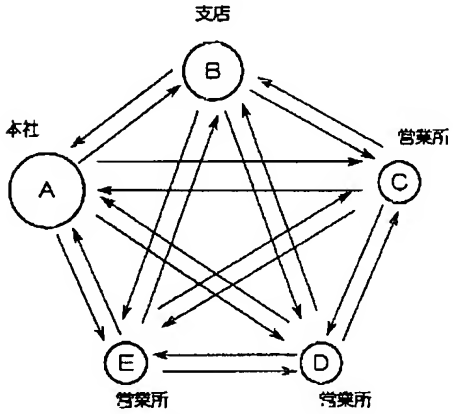
【図4】

VPN装置名	ISDN番号	グローバルIPアドレス	状態	スケジュール
A	06-4803-1111	X.X.X.X	接続	フル稼働
B	06-4804-2222	Y.Y.Y.Y	接続	七日の停止
C	06-4805-3333	Z.Z.Z.Z	接続	平日の日勤帯のみ稼動
D	06-4806-4444	V.V.V.V	切断	平日の日勤帯のみ稼動
E	06-4807-5555	W.W.W.W	切断	平日の日勤帯のみ稼動

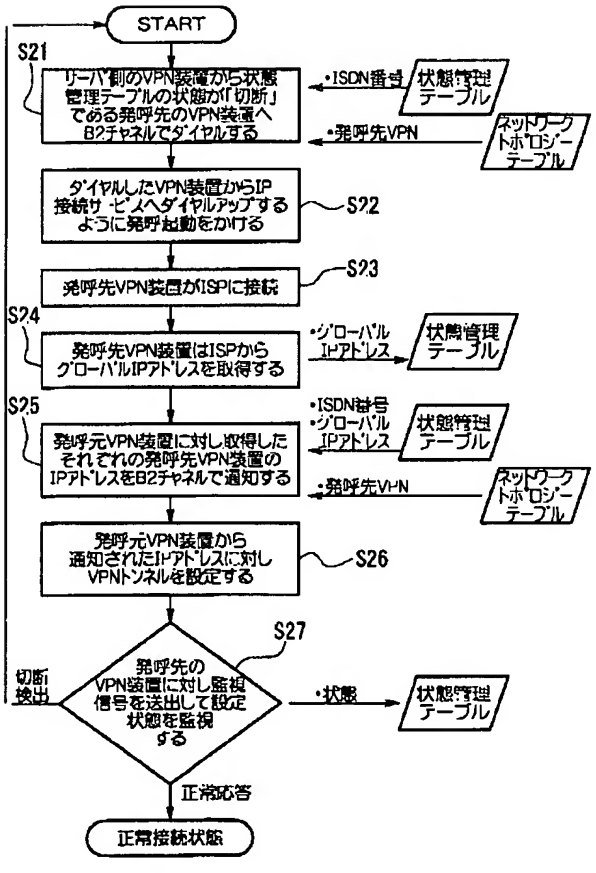
【図5】



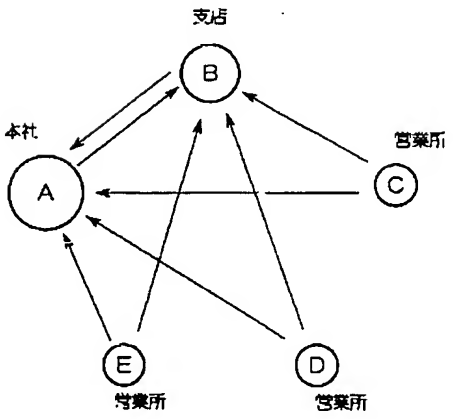
【図6】



【図7】



【図8】



フロントページの続き

(72)発明者　奥村　聡
大阪府大阪市中央区馬場町３番15号　西日本電信電話株式会社内
(72)発明者　佐藤　勝彦
大阪府大阪市中央区馬場町３番15号　西日本電信電話株式会社内

Ｆターム(参考)　5K024 AA61 CC09 CC10 GG01 GG03 GG05
5K030 GA00 HA08 HC01 HC05 HD09 KA05 KA14 MB01
5K101 KK02 KK16 LL03 LL05 MM07 PP03 QQ13 SS07 TT06 UU16